

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 9 月 2 0 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 2 7 5 9 7 3
Application Number:

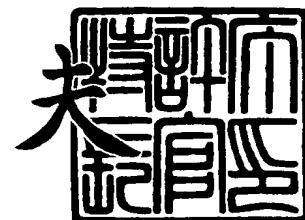
[ST. 10/C]: [J P 2 0 0 2 - 2 7 5 9 7 3]

出 願 人 株式会社リコー
Applicant(s):

2 0 0 3 年 8 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0201598

【提出日】 平成14年 9月20日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 17/60

【発明の名称】 セキュリティポリシーに基づいた文書の読み取り装置、
読み取り方法、ネットワーク配信を行う装置及びネット
ワーク配信を行う方法

【請求項の数】 32

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 斉藤 敦久

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 金井 洋一

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 谷内田 益義

【特許出願人】

 【識別番号】 000006747

 【氏名又は名称】 株式会社リコー

【代理人】

 【識別番号】 100070150

 【弁理士】

 【氏名又は名称】 伊東 忠彦

【手数料の表示】

 【予納台帳番号】 002989

 【納付金額】 21,000円

【提出物件の目録】

【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法

【特許請求の範囲】

【請求項 1】 少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、

前記読み取り方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前

記文書の読み取りを行って終了するステップと、

を有する、セキュリティポリシーに基づいた文書の読み取り方法。

【請求項2】 前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項1に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項3】 前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項1あるいは2に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項4】 前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項3に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項5】 前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項1乃至4のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項6】 請求項1乃至5のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【請求項7】 請求項6に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項8】 請求項6に記載のプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置。

【請求項9】 少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、

前記読み取り装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であることを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、
を有する、セキュリティポリシーに基づいた文書の読み取り装置。

【請求項 1 0】 前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項 9 に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 1 1】 前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 9 あるいは 1 0 に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 1 2】 前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項 1 1 に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 13】 前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項 9 乃至 12 のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 14】 少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行

可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、
を有するセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 15】 前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである、請求項 14 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 16】 前記実行対応可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 14 あるいは 15 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 17】 前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項 15 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 18】 前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項 14 乃至 17 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 19】 前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項 14 乃至 18 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 20】 前記印刷不可能なデータは、印刷禁止属性を持った PDF ファイルである、請求項 19 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 2 1】 前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項 1 4 乃至 2 0 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 2 2】 請求項 1 4 乃至 2 1 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラム。

【請求項 2 3】 請求項 2 2 に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 2 4】 請求項 2 2 に記載のプログラムをコンピュータにネットワーク配信するプログラム伝送装置。

【請求項 2 5】 少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、
を有する、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 26】 前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項 25 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 27】 前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 25 あるいは 26 に記載のセキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う装置。

【請求項 28】 前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項 27 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 29】 前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項 25 乃至 28 のうち何れか一項に記載のセキュリティポ

リシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 30】 前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項 25 乃至 29 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 31】 前記印刷不可能なデータは、印刷禁止属性を持った PDF ファイルである、請求項 30 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 32】 前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項 25 乃至 31 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う方法、装置、プログラム、記憶媒体、及び伝送装置に関連する。

【0002】

【従来の技術】

オフィスに代表されるような文書を扱うフィールドでは、その文書のセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等、特に情報のコンテナであるドキュメントに対するポリシー、中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。

【0003】

現実には多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。

【0004】

セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献1から、特許文献6）。

【0005】

例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献1）。

【0006】

また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている（特許文献2）。

【0007】

しかし、特に、上述の特許文献1では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。

【0008】

また、上述の特許文献2では、セキュリティーポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるDB（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。

【0009】**【特許文献1】**

特開 2001-184264 号公報

【特許文献2】

特開 2001-273388 号公報

【特許文献3】

特開 2 0 0 1 - 3 3 7 8 6 4 号公報

【特許文献 4】

特開平 0 9 - 2 9 3 0 3 6 号公報

【特許文献 5】

特開平 0 7 - 1 4 1 2 9 6 号公報

【特許文献 6】

特許第 0 2 7 3 5 9 6 6 号公報。

【0 0 1 0】

【発明が解決しようとする課題】

このようなセキュリティの設定方法では、文書印刷のセキュリティ設定をする場合には、第 1 に、設定者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第 2 には、すべての機器に対してセキュリティが、一つ一つ設定される必要がある。第 3 には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第 4 に、個々の機器にセキュリティ設定がされていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のような問題点がある。

本発明は、上述の問題点を解決することを目的とする。

【0 0 1 1】

特に本発明の目的は、文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の印刷装置を提供することである。

【0 0 1 2】

【課題を解決するための手段】

上記目的は、以下の本発明により解決される。

【0 0 1 3】

請求項 1 に記載の発明では、セキュリティポリシーに基づいた文書の読み取り方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性

と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、
前記読み取り方法は、
前記ユーザ属性を取得するステップと、
読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する
ステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが
許可されているか否かを、前記セキュリティポリシーに基づいて判断するステッ
プと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った
前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキ
ュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合に
は、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には
、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステッ
プと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行った
データを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前
記文書の読み取りを行って終了するステップと、
を有する。

【0014】

請求項2に記載の発明では、前記実行可能な要件は、前記読み取った文書デー
タに電子透かしを埋め込むことである。

【0015】

請求項3に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【0016】

請求項4に記載の発明では、前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0017】

請求項5に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0018】

請求項6に記載の発明は、セキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【0019】

請求項7に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0020】

請求項8に記載の発明は、そのプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置である。

【0021】

請求項9に記載の発明では、セキュリティポリシーに基づいた文書の読み取り装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、

前記読み取り装置は、
前記ユーザ属性を取得する手段と、
読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、
取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、
前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、
前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、
抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、
抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であることを判定する手段と、
実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、
すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、
を有する。

【0022】

請求項10に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【0023】

請求項11に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【0024】

請求項12に記載の発明では、前記表示可能なラベルは、少なくとも読み取り

を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0 0 2 5】

請求項 1 3 に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0 0 2 6】

請求項 1 4 に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

、
前記組み合わせでネットワーク配信を実行する場合の要件と、
を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、
を有する。

【0027】

請求項15に記載の発明では、前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである。

【0028】

請求項16に記載の発明では、前記実行対応可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【0029】

請求項17に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0030】

請求項18に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0031】

請求項19に記載の発明では、前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【0032】

請求項 20 に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持った PDF ファイルである。

【0033】

請求項 21 に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【0034】

請求項 22 に記載の発明は、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラムである。

【0035】

請求項 23 に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0036】

請求項 24 に記載の発明は、そのプログラムをコンピュータにネットワーク配信するプログラム伝送装置である。

【0037】

請求項 25 に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

、
前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、
を有する。

【 0 0 3 8 】

請求項 2 6 に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【 0 0 3 9 】

請求項 2 7 に記載の発明では、前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【 0 0 4 0 】

請求項 2 8 に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点

のタイムスタンプを含む。

【0041】

請求項29に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0042】

請求項30に記載の発明では、前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【0043】

請求項31に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持ったPDFファイルである。

【0044】

請求項32に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【0045】

以上本発明により、文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の印刷装置を提供することができる。

【0046】

【発明の実施の形態】

本発明の実施例を、図1及び図2を参照して以下に詳細に説明する。

【0047】

図1は、本発明の実施例の文書読み取り装置の構成を示す図である。また、図2は、XML (Extensible Markup Language) により記述した、本発明の実施例のセキュリティポリシーを示す。

【0048】

図1に示す本発明の実施例の文書読み取り装置100は、主に、オペレーショ

ンパネル 1 0 1、データベース 1 0 2、ユーザ属性取得手段 1 0 3、文書属性取得手段 1 0 4、セキュリティポリシー 1 0 5、読み取り手段 1 0 6、読み取りデータ 1 0 7 及びネットワークポート 1 0 8 より構成される。

【 0 0 4 9 】

オペレーションパネル 1 0 1 には、読み取り支持 1 1 0 が入力される。

【 0 0 5 0 】

図 1 においては、読み取り装置は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。また、以下に説明する本発明の実施例をコンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記録媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【 0 0 5 1 】

図 2 は、XML により記述した、セキュリティポリシーであり、つぎのようにルール 1 からルール 3 を示す。

【 0 0 5 2 】

ルール 1 は、図 2 の第 4 行目の<acc_rule>から、第 1 0 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 1 1 行目<operation>から、第 1 4 行目</operation>までの部分により記述される。

【 0 0 5 3 】

第 5 行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわらずルール 1 が適用されることを示す。

【 0 0 5 4 】

第 6 行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルが basic のときを示す。

【 0 0 5 5 】

第 9 行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわらないことを示す。

【 0 0 5 6 】

第 1 0 行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【 0 0 5 7 】

更に第 1 2 行目と第 1 3 行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【 0 0 5 8 】

従って、ルール 1 では、第 5 行目、第 6 行目、第 9 行目、第 1 0 行目、第 1 2 行目及び第 1 3 行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが” basic” の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは要件なく許可される。

【 0 0 5 9 】

次に、ルール 2 は、図 2 の第 4 行目の<acc_rule>から、第 1 0 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 1 5 行目<operation>から、第 2 0 行目</operation>までの部分により記述される。

【 0 0 6 0 】

第 5 行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール 2 が適用されることを示している。

【 0 0 6 1 】

第 6 行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【 0 0 6 2 】

第 9 行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【 0 0 6 3 】

第 1 0 行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【 0 0 6 4 】

更に、第 1 6 行目から第 1 9 行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【 0 0 6 5 】

従って、ルール 2 では、第 5 行目、第 6 行目、第 9 行目、第 1 0 行目、第 1 6 行目から第 1 9 行目により、文書カテゴリーにかかわらず、文書のセキュリティレベルが” basic” の場合には、ユーザのカテゴリーにかかわらず、且つ、ユーザのセキュリティレベルにかかわらず、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【 0 0 6 6 】

そして、ルール 3 は、図 2 の第 2 4 行目の<acc_rule>から、第 3 0 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 3 1 行目<operation>から、第 3 5 行目</operation>までの部分により記述される。

【 0 0 6 7 】

第 2 5 行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわらず示す。

【 0 0 6 8 】

第 2 6 行目の<doc_security_level>high</doc_security_level>は、文書のセキュリティレベルがhighの場合を示す。

【 0 0 6 9 】

第 2 9 行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【 0 0 7 0 】

第 3 0 行目の<user_security_level>ANY</user_security_level>は、ユーザの

セキュリティレベルにかかわりないことを示す。

【0071】

第32行目から第34行目の、

<name>scan</name>

<requirement>audit</requirement>

<requirement>embed_trace_info</requirement>

は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【0072】

従って、ルール3では、第25行目、第26行目、第29行目、第30行目、第31行目から第34行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが” high” の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【0073】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【0074】

次に、図2に示したセキュリティポリシーを使用して、図1に示した本発明の実施例の文書読み取り装置が文書を読み取り又は、読み取った文書をネットワークに配信する場合の実施例について説明する、

先ず最初に、文書読み取り装置が文書を読み取る場合の実施例について説明する。

【 0 0 7 5 】

先ず最初に、ステップ A 1 で、ユーザが、読み取り装置 1 0 0 に紙文書を設置し、オペレーションパネル 1 0 1 から、紙文書の読み取り指示 1 1 0 を入力する。

【 0 0 7 6 】

次に、ステップ A 2 で、読み取り手段 1 0 6 が、紙文書の読み取りを行う。

【 0 0 7 7 】

次に、ステップ A 3 で、文書属性取得手段 1 0 4 は、読み取った文書データのバーコードや電子透かしなどの画像情報から、文書 I D を抽出し、データベース 1 0 2 に登録されている文書 I D に対応するカテゴリ、セキュリティレベルを取得し、読み取り手段 1 0 6 に通知する。

【 0 0 7 8 】

次に、ステップ A 4 で、読み取り手段 1 0 6 は、上記の文書属性取得手段 1 0 4 が通知した文書属性に従って、セキュリティポリシー 1 0 5 の中の対応するエントリを検索して、要件を抽出する。

【 0 0 7 9 】

上述の図 2 に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが” basic” の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【 0 0 8 0 】

また、上述の図 2 に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが” high” の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【 0 0 8 1 】

次に、ステップ A 5 - 1 で、上述のステップ 4 のセキュリティレベルが” basi

c” のときの場合のように、抽出すべき要件がない場合には、読み取り手段は文書の読み取りを行って、ユーザは文書データを取得して終了する。

【0082】

一方、ステップA5-2では、上述のステップ4のキュリティレベルが” high” のときの場合のように、抽出すべき要件がある場合には、読み取り手段はその要件をすべて満たすことができるかを判定する。

【0083】

ステップA5-2の場合には、次に以下のステップ6-1と6-2が実行される。

【0084】

ステップA6-1では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【0085】

次に、ステップA6-2では、すべての要件を満たすことができる場合は、その要件を満たした読み取りを行って、ユーザは文書データを取得して終了する。この場合には、ステップA6-2では、以下のステップ、A7-1からA7-6が実行される。

【0086】

ステップA7-1では、ユーザ属性取得手段103は、オペレーションパネル101から読み取り指示110を出したユーザに、ユーザIDの入力要求を出す。

【0087】

次に、ステップA7-2では、ユーザは、オペレーションパネル101からユーザIDを入力する。

【0088】

次に、ステップA7-3では、ユーザ属性取得手段103は、ユーザIDからデータベース102に登録されている入力されたユーザIDに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段106に通知する。

【0089】

次に、ステップA7-4では、ログを記録する。

【0090】

そして、ステップA7-5では、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【0091】

最後に、ステップA7-6で、ユーザは文書データを、読み取りデータ107内に取得して終了する。

【0092】

以上のように、図2に示したセキュリティポリシーを使用して、図1に示した本発明の実施例の文書読み取り装置が文書を読み取ることができる。

【0093】

次に、文書読み取り装置が文書を読み取り且つ読み取った文書をネットワークに配信する場合の実施例について説明する。

【0094】

先ず最初に、ステップB1で、ユーザが、読み取り装置106に紙文書をセットし、オペレーションパネル106から、読み取りデータの配信先の指定及び紙文書の読み取り指示110を出す。

【0095】

次に、ステップB2で、読み取り手段106が、紙文書の読み取りを行う。

【0096】

次に、ステップB3で、文書属性取得手段104は、読み取った文書データのバーコードや電子透かしなどの画像情報から文書IDを抽出し、データベース102に登録されている文書IDに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段106に通知する。

【0097】

次に、ステップB4では、読み取り手段106は、上記の文書属性取得手段104が通知した文書属性に従って、セキュリティポリシー105の中の対応する

エントリを検索し、要件を抽出する。

【0 0 9 8】

上述の図 2 に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが” basic” の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【0 0 9 9】

また、上述の図 2 に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが” high” の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと（例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など）」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【0 1 0 0】

次に、例えば、文書をネットワークへ配信する際の要件が、セキュリティポリシー 1 0 5 内に存在しない場合には、ステップ B 5 - 1 では、読み取り手段 1 0 6 は文書をネットワークポート 1 0 8 を介してネットワークへ配信して、処理を終了する。

【0 1 0 1】

一方、例えば、文書をネットワークへ配信する際の要件が、セキュリティポリシー 1 0 5 内に存在する場合には、ステップ 5 - 2 で、読み取り手段 1 0 6 が、その要件をすべて満たすことができるかを判定する。

【0 1 0 2】

ステップ B 5 - 2 の場合には次に、ステップ B 5 - 3 で、ネットワークに配信することを許可するルールがない場合には、読み取り手段 1 0 6 が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、読み取りデータを破棄して終了する。例えば、これは、上述のステップ B 4 の、セキュリティレベルが” high” の場合である。

【0103】

次に、ステップB6-1では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【0104】

次に、ステップB6-2では、例えば、上述のセキュリティレベルが” basic ” の場合のように、すべての要件を満たすことができる場合は、その要件を満たした読み取り及び、文書をネットワークに配信して終了する。この場合には、ステップB6-2では、以下のステップ、B7-1からB7-6が実行される。

【0105】

ステップB7-1では、ユーザ属性取得手段106は、オペレーションパネル101から、読み取り指示110を出したユーザに、ユーザIDの入力要求を出す。

【0106】

次に、ステップB7-2では、ユーザは、オペレーションパネル101からユーザIDを入力する。

【0107】

次に、ステップB7-3では、ユーザ属性取得手段103は、ユーザIDからデータベース102に登録されている入力されたユーザIDに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段106に通知する。

【0108】

次に、ステップB7-4では、ログを記録する。

【0109】

そして、ステップB7-5では、読み取った文書データを、印刷不可能なデータ(たとえばADOBE(登録商標)の印刷禁止属性を持ったPDFなど)に変換する。

【0110】

最後にステップB7-6では、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、文書を、ネットワークポート108を介してネットワークへ配信し、終了する。

【0111】

以上のように、図 2 に示したセキュリティポリシーを使用して、図 1 に示した本発明の実施例の文書読み取り装置が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【0112】

【発明の効果】

以上説明したように、本発明によって、セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、及び伝送装置を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の実施例の文書読み取り装置の構成を示す図である。

【図 2】

XML (Extensible Markup Language) により記述した、本発明の実施例のセキュリティポリシーを示す図である。

【符号の説明】

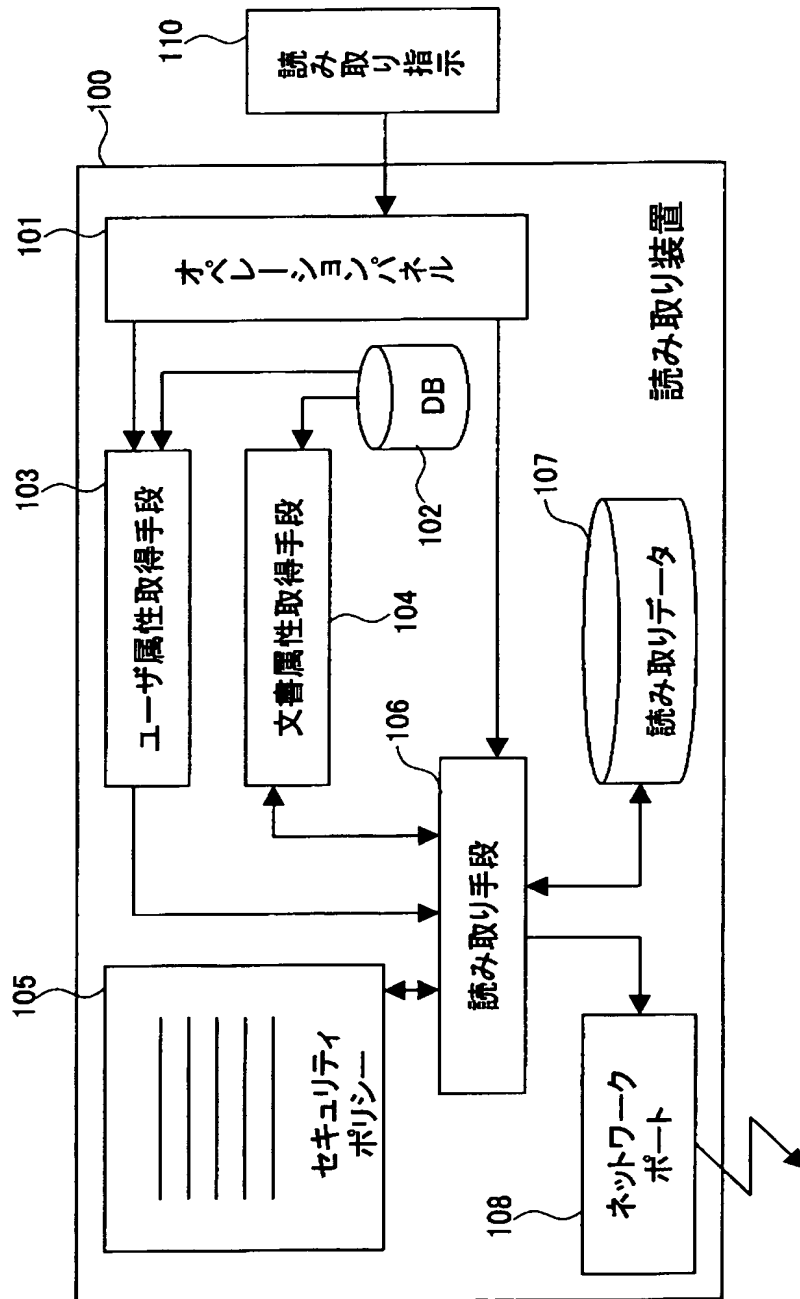
- 100 文書読み取り装置
- 101 オペレーションパネル
- 102 データベース
- 103 ユーザ属性取得手段
- 104 文書属性取得手段
- 105 セキュリティーポリシー
- 106 読み取り手段
- 107 読み取りデータ
- 108 ネットワークポート
- 110 読み取り指示

【書類名】

図面

【図 1】

本発明の実施例の文書読み取り装置の構成を示す図



【図 2】

XML(Extensible Markup Language)により記述した
本発明の実施例のセキュリティポリシーを示す図

```

<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
<acc_rule>
<doc_category>ANY</doc_category>
<doc_security_level>basic</doc_security_level>
<acl>
<ace>
<user_category>ANY</user_category>
<user_security_level>ANY</user_security_level>
<operation>
<name>scan</name>
<allowed/><!-- allowed without any requirement -->
</operation>
</operation>
<name>net_delivery</name>
<requirement>audit</requirement>
<requirement>print_restriction</requirement>
<requirement>trusted_channel</requirement>
</operation>
</ace>
</acl>
</acc_rule>
</acc_rule>
<doc_category>ANY</doc_category>
<doc_security_level>high</doc_security_level>
<acl>
<ace>
<user_category>DOC-CATEGORY</user_category>
<user_security_level>ANY</user_security_level>
<operation>
<name>scan</name>
<requirement>audit</requirement>
<requirement>embed_trace_info</requirement>
</operation>
</ace>
</acl>
</acc_rule>
</policy>

```

【書類名】 要約書

【要約】

【課題】 文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法を提供する。

【解決手段】 ユーザ属性を取得し、文書属性を取得し、ユーザ属性と文書属性との組み合わせに対して読み取りが許可されているかをセキュリティポリシーにより判断し、許可されていない場合にはデータを破棄して終了し、許可されている場合には対応する要件をセキュリティポリシーから抽出し、要件がセキュリティポリシー内に存在しない場合には文書の読み取りを行って終了し、要件がセキュリティポリシー内に存在する場合にはすべての要件を読み取る方法で実行可能であるかを判定し、実行可能でない要件が存在する場合にはデータを破棄して終了し、すべての要件を実行可能である場合には抽出された前記要件を満たして文書の読み取りを行って終了する、セキュリティポリシーに基づいて文書を読み取る方法により実現する。

【選択図】 図 1

特願 2 0 0 2 - 2 7 5 9 7 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日 1 9 9 0 年 8 月 2 4 日
 [変更理由] 新規登録
 住 所 東京都大田区中馬込 1 丁目 3 番 6 号
 氏 名 株式会社リコー

2. 変更年月日 2 0 0 2 年 5 月 1 7 日
 [変更理由] 住所変更
 住 所 東京都大田区中馬込 1 丁目 3 番 6 号
 氏 名 株式会社リコー